CLAIM AMENDMENTS

The following claim listing replaces all previous versions of the claims.

Claim Amendment Summary

Claims pending

- Before this Amendment: Claims 1-20 and 26-38.

- After this Amendment: Claims 1-6, 8-20 and 26-38

Non-Elected, Canceled, or Withdrawn claims: 7, 21-25 and 39-43

Amended claims: 1-20 and 26-38

New claims: none

Claims:

Serial No.: 10/625,363
Atty Docket No.: MS1-1285US
Atty/Agent: Beatrice L. Koempel-Thomas
RESPONSE TO FINAL OFFICE ACTION

3

lee&hayes The Business of IP™
www.leehayes.com   509.324.9256

1.   (Currently Amended) A computer-readable medium having computer-executable instructions that, when executed by a computer, performs a method for protecting digital media comprising:

obtaining a message M having two portions, wherein M_1 is one of the portions of the M and M_2 is another;

generating one or more codes having a combination with M_2 implicitly embedded therein, wherein calculations that generate the one or more codes do not employ M_2 or an encryption of M_2, and M_2 cannot be derived from these calculations of one or more codes, the generating further comprising:

finding a value of a variable per-message key (k) where a predefined mathematical function, $M_2 = H_0(M_1, g^k)$, employing k produces a result equivalent to M_2, wherein g is a fixed element of order q in a fixed group, and H_0 is a predefined hash function instantiated by using a keyed version of a secure hash function; and

when such a value of k is found, calculating two or more codes, where the calculation of one code is not identical to the calculation of any other code and where each calculation incorporates k; and

reporting the one or more codes, by which reporting the one or more codes facilitates a cryptographic technique for protecting digital media.

2. (Currently Amended) [[A]] The medium as recited in claim 1, wherein the method further comprises producing a digital signature (*DS*) comprising M_1 and the reported one or more codes.

Serial No.: 10/625,363
Atty Docket No.: MS1-1285US
Atty/Agent: Beatrice L. Koempel-Thomas
RESPONSE TO FINAL OFFICE ACTION

4

lee&hayes   The Business of IP™
www.leehayes.com   509.324.9256

3. **(Currently Amended)** [[A]] <u>The</u> medium as recited in claim 1, wherein two or more codes are generated by the generating and reported by the reporting.

4. **(Currently Amended)** [[A]] <u>The</u> medium as recited in claim 3, wherein a mathematical function for calculating one code is not identical to a mathematical function for calculating another code.

5. **(Currently Amended)** [[A]] <u>The</u> medium as recited in claim 3, wherein the message M has a ~~defined~~ <u>pre-determined</u> length and a length of a combination of two or more codes is less than the message's ~~defined~~ <u>pre-determined</u> length.

6. **(Currently Amended)** [[A]] <u>The</u> medium as recited in claim 3, wherein M_2 has a ~~defined~~ <u>pre-determined</u> length and a length of a combination of two or more codes is less than or equal to the ~~defined~~ <u>pre-determined</u> length of M_2.

7. **(Canceled)**

8. **(Currently Amended)** [[A]] <u>The</u> medium as recited in claim 1, wherein the generating comprises:

finding a value of a variable per-message key (k) where a predefined mathematical function, $M_2 = H_0(M_1, g^k)$, employing k produces a result equivalent to M_2, wherein g is a fixed element of order q in a fixed group, and H_0 is a predefined hash function instantiated by using a keyed version of a secure hash function;

when such a value of k is found, calculating the two or more codes, where the calculation of one code is not identical to the calculation of any other code, the calculation of at least one code employs non-linear mathematical function, and where each calculation incorporates k.

9. (Currently Amended) [[A]] <u>The</u> medium as recited in claim 3, wherein the generating comprises:

finding a value of a variable per-message key (k) where a predefined mathematical function, $M_2 = H_0(M_1, g^k)$, employing M_1 and g^k produces a result equivalent to M_2, wherein g is a fixed element of order q in a fixed group, and H_0 is a predefined hash function instantiated by using a keyed version of a secure hash function;

when such a value of k is found, calculating the two or more codes, where one code is r and another is s, with r being calculated using another predefined mathematical function employing M_1 and g^k, <u>$r = H_1 (M_1, g^k)$,</u> and with s being calculated using still another predefined mathematical function employing M_1 and g^k and r, <u>$s = k/(r + 1) - x$ $H_2 (M_1, g^k)$mod q</u>.

10. (Currently Amended) [[A]] <u>The</u> medium as recited in claim 3, wherein the method further comprises producing a digital signature (*DS*) comprising M_1 and the reported codes.

11. (Currently Amended) A computing device comprising:

an output peripheral device;

[[a]] <u>the</u> medium as recited in claim 1.

12. **(Currently Amended)** A computer-readable medium having computer-executable instructions that, when executed by a computer, performs a method comprising:

obtaining a message M having two portions, wherein M_1 is one of the portions of the M and M_2 is another;

generating two or more codes having a combination with M_2 implicitly embedded therein, wherein calculations that generate the codes do not employ M_2 or an encryption of M_2, and M_2 cannot be derived from these calculations of ~~one~~ two or more codes, wherein the generating comprises:

- finding a value of a variable per-message key (k) where a predefined mathematical function, $M_2 = H_0(M_1, g^k)$, employing M_1 and g^k produces a result equivalent to M_2, wherein g is a fixed element of order q in a fixed group, and H_0 is a predefined hash function instantiated by using keyed versions of a secure hash function;

- when such a value of k is found, calculating the two or more codes, ~~where the calculation of one code is not identical to the calculation of any other code and where each calculation incorporates k;~~ where one code is r and another is s, with r being calculated using another predefined mathematical function employing M_1 and g^k, $r = H_1(M_1, g^k)$, and with s being calculated using still another predefined mathematical function employing M_1 and g^k and r, $s = k/(r + 1) - x\,H_2(M_1, g^k)\bmod q$;

reporting the two or more codes, by which reporting the two or more codes facilitates a cryptographic technique for protecting digital media.

13.   (Currently Amended) [[A]] The medium as recited in claim 12, wherein the method further comprises producing a digital signature (*DS*) comprising M_1 and the reported two or more codes.

14.   (Currently Amended) [[A]] The medium as recited in claim 12, wherein the calculation of at least one code employs a non-linear mathematical function.

15.   (Currently Amended) [[A]] The medium as recited in claim 12, wherein the message *M* has a ~~defined~~ pre-determined length and a length of a combination of two or more codes is less than the message's ~~defined~~ pre-determined length.

16.   (Currently Amended) [[A]] The medium as recited in claim 12, wherein M_2 has a ~~defined~~ pre-determined length and a length of a combination of two or more codes is less than or equal to the ~~defined~~ pre-determined length of M_2.

17.   (Currently Amended) [[A]] The medium as recited in claim 12, wherein one calculated code is *r* and another is *s*, with *r* being calculated using another predefined mathematical function employing M_1 and g^k, and with *s* being calculated using still another predefined mathematical function employing M_1 and g^k and *r*.

18. (Currently Amended) [[A]] The medium as recited in claim 17, wherein the predefined mathematical function for s is non-linear.

19. (Currently Amended) [[A]] The medium as recited in claim 17, wherein the method further comprises producing a digital signature (DS) comprising M_1 and the reported codes r and s.

20. (Currently Amended) A computing device comprising:

an output peripheral device;

[[a]] the medium as recited in claim 12.

21-25. (CANCELED)

26. (Currently Amended) A method for facilitating digital security, the method comprising:

obtaining a message M having two portions, wherein M_1 is one of the portions of the M and M_2 is another;

generating two or more codes having a combination with M_2 implicitly embedded therein, wherein calculations that generate the codes do not employ M_2 or an encryption of M_2, and M_2 cannot be derived from these calculations of one or more codes, wherein the generating comprises:

- finding a value of a variable per-message key (k) where a predefined mathematical function, $M_2 = H_0(M_1, g^k)$, employing M_1 and g^k produces a result equivalent to M_2, wherein g is a fixed element of order q in a fixed

Serial No.: 10/625,363
Atty Docket No.: MS1-1285US
Atty/Agent: Beatrice L. Koempel-Thomas
RESPONSE TO FINAL OFFICE ACTION

9

lee&hayes   The Business of IP™
www.leehayes.com   509.324.9256

group, and H_0 is a predefined hash function instantiated by using keyed versions of a secure hash function;

- when such a value of k is found, calculating the two or more codes, where the calculation of one code is not identical to the calculation of any other code and where each calculation incorporates k;

reporting the two or more codes, by which reporting the two or more codes facilitates a cryptographic technique for protecting digital media.

27. **(Currently Amended)** [[A]] The method as recited in claim [[1]] 26 further comprising producing a digital signature (*DS*) comprising M_1 and the reported two or more codes.

28. **(Currently Amended)** A digital signature (*DS*) produced by [[a]] the method as recited in claim 27 and embodied on a computer-readable medium.

29. **(Currently Amended)** A digital signature (*DS*) produced by [[a]] the method as recited in claim 27 and embodied as human-readable indicia on a human-readable medium.

30. **(Currently Amended)** [[A]] The method as recited in claim [[1]] 26, wherein the calculation of at least one code employs a non-linear mathematical function.

31. (Currently Amended) [[A]] The method as recited in claim [[1]] 26, wherein the message M has a ~~defined~~ pre-determined length and a length of a combination of two or more codes is less than the message's ~~defined~~ pre-determined length.

32. (Currently Amended) [[A]] The method as recited in claim [[1]] 26, wherein M_2 has a ~~defined~~ pre-determined length and a length of a combination of two or more codes is less than or equal to the ~~defined~~ pre-determined length of M_2.

33. (Currently Amended) [[A]] The method as recited in claim [[1]] 26, wherein one calculated code is r and another calculated code is s, with r being calculated using another predefined mathematical function employing M_1 and g^k, $r = H_1 (M_1, g^k)$, and with s being calculated using still another predefined mathematical function employing M_1 and g^k and r, $s = k/(r + 1) - x H_2 (M_1, g^k) \bmod q$.

34. (Currently Amended) [[A]] The method as recited in claim 33, wherein the predefined mathematical function for s is non-linear.

35. (Currently Amended) [[A]] The method as recited in claim 33, wherein the predefined mathematical function for s is quadratic.

36. (Currently Amended) [[A]] The method as recited in claim [[1]] 26 further comprising producing a message comprising M_1 and the reported codes.

Serial No.: 10/625,363
Atty Docket No.: MS1-1285US
Atty/Agent: Beatrice L. Koempel-Thomas
RESPONSE TO FINAL OFFICE ACTION

11

lee&hayes   The Business of IP™
www.leehayes.com   509.324.9256

37. **(Currently Amended)** A computer-readable medium embodying a message produced by [[a]] the method as recited in claim 36, by which the message functions with a processor to protect digital media.

38. **(Currently Amended)** A method comprising:

producing a message produced by [[a]] the method as recited in claim 36 as human-readable indicia on a human-readable medium.

39-43. **(CANCELED)**